Information Technology Resource Management Documents

ITRM Policy SEC 500-02: Information Technology Security Policy

Presented to the ITIB

July 19, 2006

Presentation Outline

- Scope of the Policy
- Purpose of the Policy
- Policy Development
- Policy Guiding Principles
- Policy Overview
- Related Documents & Timelines
- Questions

Scope of ITRM Policy SEC500-02

- This policy is applicable to all State agencies and institutions of higher education that manage, develop, purchase, and use information technology resources in the Commonwealth.

- However, academic “instruction or research” systems are exempt from this policy provided they are not subject to a State or Federal Law/Act mandating security due diligence. This policy is offered only as guidance to local government entities.

Purpose of ITRM Policy SEC500-02

- To protect the Commonwealth information technology assets and the information processed by defining the minimum information technology security program for agencies of the Commonwealth of Virginia (COV).
- It remains the policy of the COV that each Agency Head is responsible for the security of the Agency's data and having appropriate steps taken to secure Agency IT systems and data through the development of an Agency IT security program.

Policy Development

- Policy directions were developed by a collaborative effort that involved input from a security workgroup comprised of:
  - Staff from VITA divisions including Security and Policy, Practice and Architecture;
  - Executive Branch Agencies Information Security Offices (ISOs) including Institutions of Higher Education and staff from the Auditor of Public Accounts; and
  - Other Executive Branch Agencies via VITA’s online review and comment application (ORCA).

Policy Guiding Principles

COV Data is:

- A critical asset that shall be protected; and
- Restricted to authorized personnel for official use.

IT security must be:

- A cornerstone of maintaining public trust;
- Managed to address both business and technology requirements;
- Risk-based and cost-effective;
- Aligned with COV priorities, industry-prudent practices, and government requirements;
- Directed by policy but implemented by business owners;
- The responsibility of all users of COV IT systems and data.

Policy Overview

- The Policy Addresses:
  - Key IT Security Roles and Responsibilities
  - IT Security Program Components
  - Compliance Monitoring
  - IT Security Audits
  - Protection of IT Resources
  - Process for Requesting Exception to the IT Security Policy

Related Documents & Timelines

- ITRM Standard SEC501-01: Information Technology Security Standard
  - Effective July 1, 2006
  - Compliance July 1, 2007
- ITRM Standard SEC502-00: Information Technology Security Audit Standard
  - Effective July 1, 2006
  - Compliance February 1, 2007
- Guidelines and workshops for implementing a compliant IT security program.
  - Dates to be announced.

QUESTIONS?

Recommendation

Move that *ITRM Policy SEC500-02: Information Technology Security Policy* be recommended for approval by the full ITIB.